Electronic Version

Stylesheet Version v1.1.1

CRYPTO-SYSTEM WITH AN INVERSE KEY EVALUATION CIRCUIT

Abstract

An inverse key evaluation circuit for inversely generating a plurality of pre-keys in sequence according to an original key, and a crypto-system containing the inverse key evaluation circuit for decrypting a ciphered text into a plain text according to the plurality of pre-keys. The inverse key evaluation circuit includes a key-receiving module and an inverse key evaluation module. The key-receiving module includes a register for temporally receiving and storing the original key, which will be processed by the inverse key evaluation module to generate the plurality of pre-keys of the original key.The key stored in the register will then be replaced by the newly generated pre-key in sequence. The crypto-system includes a key-generating module that contains the inverse key evaluation circuit, an encryption module, and a decryption module.